BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-215

1 AUGUST 1996
Communications and Information

★*CONTROLLING AUTHORITIES FOR COMSEC KEYING MATERIAL*

NOTICE: This publication is available digitally. Contact your Publishing Distribution Office (PDO) for the monthly CD-ROM or access to the bulletin board system. The target date for discontinuing paper publications is December, 1996.

This instruction outlines responsibilities of personnel who control (controlling authorities) communications security (COMSEC) keying material. It describes the roles of Headquarters Air Force Communications Agency (HQ AFCA), San Antonio Air Logistics Center (SA-ALC), Director, Cryptologic Management (SA-ALC/LTMKK) and the National Security Agency (NSA) in controlling COMSEC keying material. It also implements National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4006 (FOUO), *Controlling Authorities for COMSEC Material*. It takes precedence over all other Air Force publications affecting COMSEC controlling authorities. Send recommended changes to HQ AFCA, Information Protection Division (AFCA/SYS), Scott AFB IL 62225-5234. Refer conflicts between this and other instructions to HQ AFCA, Doctrine, Policy, Procedures Branch (HQ AFCA/XPPD), on AF Form 847, **Recommendation for Change of Publication**, with an information copy to Headquarters United States Air Force , Information Warfare Division (HQ USAF/SCTW), 1250 Air Force Pentagon, Washington DC 20330-1250. Major commands (MAJCOM), field operating agencies (FOA), and direct operating units (DRU) send one copy of their supplement to HQ USAF/SCTW, HQ AFCA/SYS, and HQ AFCA/XPPD.

SUMMARY OF REVISIONS

This revision updates the entire document.

1. Introduction. This instruction assigns responsibilities to controlling authorities for keying material. It describes functions and lists options for reacting to emergency or crisis situations and tells how to evaluate COMSEC incidents. The term MAJCOM when used in this publication, includes FOAs and DRU. A glossary of references, abbreviations, acronyms, and terms is at attachment 1.

2. Applicability and Scope. This instruction applies to all Air Force personnel assigned or acting as, controlling authorities to oversee and manage operational use and control of COMSEC keying material, Communications-Electronics Operation Instructions (CEOI), Joint Communications-Electronics Operation Instructions (JCEOI), and Signal Operation Instructions (SOI). Although by definition CEOIs, JCEOIs, and SOIs are not keying material, they are included in this instruction to define the responsibilities of controlling authorities for these items. Manages positive control material according to CJCSI 3260.01 (S), *Joint Policy Governing Positive Control Material and Devices (U)*

3. Objectives
3.1. Make sure of proper authorization, control, and management of COMSEC keying material.
3.2. Set up an orderly structure by assigning responsibilities for evaluating COMSEC incident reports.

4. Controlling Authority Appointment. The MAJCOM or agency that sets up the new cryptonet identifies a controlling authority to oversee and manage the operational use and control of keying material. Normally, the next higher level to cryptonet members performs the controlling authority roles, even if the controlling authorities are not organizationally senior to cryptonet members. All cryptonet members, including those from other services or agencies, must follow directions given

Supersedes: AFI 33-215, 18 November 1994.
OPR: HQ AFCA/SYSC (Msgt Perkins)
Certified by: HQ USAF/SCXX (Colonel Brian D. Miller)
Pages: 9/Distribution: F

by the controlling authority. Do not assign the COMSEC account as the controlling authority for keying material. SA-ALC/LTMKK specifies the initial cryptonet activation and key implementation date, unless otherwise directed by controlling authorities. **NOTE**: MAJCOM COMSEC offices will not be assigned as controlling authorities.

4.1. For electronically generated key, the organization directing key generation does the controlling authority functions, unless those functions are specifically assigned to another organization.

4.2. The Joint Staff, the chiefs of the military services, the commanders of the unified and specified commands, the heads of departments and agencies, and MAJCOMs may direct changes in controlling authority appointments under their control. Whoever directs these changes notifies all cryptonetmembers, appropriate distribution authorities, and Director, National Security Agency (DIRNSA)/Y13), of all controlling authority appointments and changes.

4.3. Set up a controlling authority for each CEOI, JCEOI, or SOI system. The controlling authority for MAJCOM CEOIs, JCEOIs, and SOIs is the MAJCOM commander or their appointed representative.

5. Cryptonet Management . Procedures for cryptonet management are in attachment 2. Controlling authorities are allowed direct communications with cryptonet members. Controlling authorities must keep accurate records of the cryptonet in order to assess the impact of, and recover from, a compromise. This includes:

5.1. Cryptonet member identities and the amount of keying material they hold.

5.2. Logistics support and resupply requirements for the cryptonet.

5.3. Cryptoperiod extensions allowed.

5.4. Cryptonet activation and key implementation dates.

5.5. Operational requirements for the cryptonet.

5.6. Key change (HJ) time.

5.7. Spare group assignments for codes and authenticators.

5.8. Any extracts or local copying of keying material allowed.

6. SA-ALC Responsibilities:

6.1. Act as the central office of record for all Air Force COMSEC accounts.

6.2. Provide overall management support for COMSEC material held by Air Force, Defense Logistics Agency, and Federal Aviation Administration COMSEC accounts.

6.3. Send out urgent messages to COMSEC accounts, MAJCOMs, and other concerned commands/agencies using MAJCOM address indicator groups or direct to COMSEC accounts to include:

6.3.1. Notices of compromised or replaced COMSEC material, including disposition instructions, when applicable.

6.3.2. Instructions for making encrypted-traffic reviews because of declared compromises of COMSEC material.

6.3.3. Notices of non-routine supersession and changes of effective date.

6.3.4. COMSEC publication amendments that require immediate implementation.

6.3.5. Other procedural and operational changes when immediate action is necessary.

7. HQ AFCA Responsibilities:

7.1. Act as USAF COMSEC Incident Management Office.

7.2. Evaluate all reported physical COMSEC incidents involving multiple Air Force controlling authorities.

8. Controlling Authority Responsibilities.

8.1. Cryptonet Controlling Authorities:

8.1.1. Tell SA-ALC/LTMKK, NSA, and all cryptonet members of appointment as controlling authority and changes (see attachment 3 for the role of NSA.).

8.1.2. Approve changes in classification of the key if the classification is to be downgraded. Any upgrades to the classification must first be coordinated with SA-ALC/LTMKK.

8.1.3. Review and send evaluations of COMSEC incidents to all addressees of the initial COMSEC incident report.

8.1.3.1. Evaluate or respond to initial reports of the following incidents within 24 hours:

8.1.3.1.1. Currently effective keying material or keying material that is effective within 15 days.

8.1.3.1.2. Defection, espionage, hostile cognizant agent, clandestine exploitation, tampering, penetration or sabotage, or unauthorized copying, reproduction, or photography.

8.1.3.2. Evaluate or respond to initial reports of the following incidents within 48 hours:

8.1.3.2.1. Future keying material that becomes effective beyond the next 15 days.

8.1.3.2.2. Superseded, reserve, or contingency keying material.

8.1.3.3. Evaluate or respond to initial reports of COMSEC incidents not covered above within 5 duty days.

8.1.4. Direct the emergency supersession of keying material under their control according to AFI 33-212, *Reporting COMSEC Incidents*, and immediately notify SA-ALC/LTMKK and DIRNSA/Y13.
8.1.5. Coordinate with SA-ALC/LTMKK prior to superseding key to make sure adequate material is available to support future needs.
8.1.6. Direct the emergency extension of keying material under their control when necessary (attachments 2 and 4).
8.1.7. Direct a record traffic review for the time period involved when cryptonet keying material is compromised.
8.1.8. Additionally, they:
8.1.8.1. Coordinate actions to establish contingency keying material with the SA-ALC.
8.1.8.2. Recommend changes in manual cryptosystems content and format to HQ AFC4A/SYS.
8.1.8.3. Perform cryptonet management as outlined in attachment 2.
8.1.8.4. Report COMSEC incidents according to AFI 33-212.
8.1.8.5. Evaluate COMSEC incidents according to the guidelines in AFI 33-212.
8.2. CEOI, JCEOI, and SOI Controlling Authorities:
8.2.1. Announce implementation of the system and inform DIRNSA/Y13 of the supersession and projected usage.
8.2.2. Update requirements to DIRNSA/V32 in a timely manner.
8.2.3. Recommend changes in content, format, or classification to DIRNSA/V32.
8.2.4. Allow the extension of the effective period to suit operational conditions. These extensions are not reportable to NSA.
8.2.5. Evaluate incidents according to AFI 31-401, *Managing the Information Security Program*. Incidents involving CEOIs, JCEOIs, and SOIs are not reportable to NSA.
8.2.6. Direct emergency supersession and notify DIRNSA/V32/Y13 for resupply action.

JOHN S.FAIRFIELD, Lt General, USAF
DCS/Communications and Information

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

References

AFI 33-212, *Reporting COMSEC Incidents*
AFI 33-216, *Management of Manual Cryptosystems*
AFI 31-401, *Managing the Information Security Program*
AFKAG-2, *Air Force COMSEC Accounting Manual*
CJCSI 3260.01(S), Joint Policy Governing Positive Control Material and Devices (U)
NSTISSI No. 4006 (FOUO), Controlling Authorities for COMSEC Material

Abbreviations and Acronyms

AFI−Air Force Instruction
AIG−Address Indicator Group
CEOI−Communications-Electronics Operating Instruction
COMSEC−Communications Security
CSS−Coded Switch System
DIRNSA−Director, National Security Agency
DRU−Direct Reporting Unit
FOA−Field Operating Agency
DSN−Defense Switched Network
HJ−Key Change
HQ AFCA−Headquarters, Air Force Communications Agency
HQ USAF−Headquarters, United States Air Force
JCEOI−Joint Communications-Electronics Operating Instruction
JCS−Joint Chiefs of Staff
JS−Joint Staff
KEK−Key Encryption Key
MAJCOM−Major Command
NCCD−Nuclear Certified Computer Data
NSA−National Security Agency
NSTISSI−National Security Telecommunications and Information SystemsSecurity Instruction
PAL−Permissive Action Link
PES−Positive Enable System
SA-ALC−San Antonio Air Logistic Center
SAS−Sealed Authenticator Systems
SOI−Signal Operating Instruction
STU-III−Secure Telephone Unit III

Terms

COMSEC Incident—Any occurrence that has the potential to jeopardize the security of COMSEC material or the secure electrical transmission of national security information.
COMSEC Incident Monitoring Activity—The office within a department or agency that maintains a record of COMSEC activity incidents caused by elements of that department or agency and makes sure all actions required of those elements are completed (HQ AFC4A/SYSC for the Air Force).
Cryptonet—Stations that hold a specific key for use. *NOTE: Activities holding a key for other than use, such as cryptologic depots, are not cryptonet members for that key. Controlling authorities are actual members of the cryptonets they control.*
Cryptonet member—An individual station, among a group of stations, holding a specific key for use. Controlling authorities are defacto cryptonet members.
JCS Positive Control Material—A generic term referring to Sealed Authenticator Systems (SAS), Permissive and Action Link (PAL), Coded Switch System (CSS), Positive Enable System (PES), and Nuclear Certified Computer Data (NCCD).

PROCEDURES FOR CRYPTONET MANAGEMENT

A2.1. Controlling Authority. Controlling authorities appoint and keep a record of cryptonet members and prescribe the quantity of keying material for each member. This requires:

A2.1.1. Knowing the identity of all cryptonet members and the problems users may experience with the keying material.

A2.1.2. Knowing the distribution authorities that support the holders of the material and the fastest ways of issuing supersession and other emergency information to all holders of the keying material.

A2.1.3 Making sure cryptonet members know they require training to recognize COMSEC incidents and reporting procedures to the COMSEC manager.

A2.2. Logistics Support. Controlling authorities coordinate the establishment and logistics support of cryptonets with SA-ALC/LTMKK and advise SA-ALC/LTMKK of COMSEC accounts and the quantity of keying material needed. For manual cryptosystems (one-time pads, operations codes, authentication systems, etc.), controlling authorities must first identify specific operational requirements to HQ AFC4A/SYS according to AFI 33-216, *Management of Manual Cryptosystems*. Serious consideration must be given to use of the automanual (KL-43) and/or machine crypto system rather than requesting a paper-based system (codes, authenticators).

A2.3. Resupply. Controlling authorities coordinate with distribution authorities to make sure of timely resupply of keying material. Controlling authorities must:

A2.3.1. Promptly check the status of follow-on material when COMSEC accounts have only a 2-month supply of keying material--except annually superseded material.

A2.3.2. Direct users to implement the longest authorized cryptoperiod extension for each remaining key setting if COMSEC accounts cannot be assured of resupply before their remaining key is expended (paragraph A2.4).

A2.3.3. If the extension is not enough or the resupply date is not determined, controlling authorities must report, by IMMEDIATE precedence message, to SA-ALC/LTMKK, INFO: DIRNSA/V51/Y13. This allows responsible agencies to make contingency arrangements. The message must include:

A2.3.3.1. The keying material short title.

A2.3.3.2. Number of cryptonet members.

A2.3.3.3. Description of the type of operations (for example, full-time, or part-time, fixed or mobile communications center).

A2.3.3.4. Explanation of the necessity for the cryptoperiod extension.

NOTE: When time is critical, controlling authorities may verbally request emergency cryptoperiod extensions from DIRNSA/V51(DSN/STU-III 644-0111) extension 859-6804; commercial/STU-III (410) 859-6804. When authorized verbally, controlling authorities must take immediate action and not wait for message documentation. Cryptonet members abide by verbal instructions relayed by controlling authorities.

A2.4. Extensions. Controlling authorities for manual cryptosystems can extend the cryptoperiod by 72 hours. Controlling authorities for automanual and machine cryptosystems can extend the cryptoperiod by 1 week. That is, controlling authorities can add either 72 hours or 1 week, as applicable, to the regular cryptoperiod, unless the specific cryptosystem doctrine prohibits cryptoperiod extensions or authorizes a longer extension. Controlling authorities are not required to report these extensions to SA-ALC or NSA. Cryptonet members can extend cryptoperiods up to 2 hours to complete a transmission or conversation in process at HJ time. Controlling authority approval is not required and net members are not required to report these extensions. See attachment 4, Guidelines For Extending Cryptoperiods. Controlling authorities can approve indefinite cryptoperiod extensions for CEOI/JCEOI/SOI.

A2.5. Activating a Cryptonet. SA-ALC specifies initial cryptonet activation and key implementation date unless otherwise directed by the controlling authority. The controlling authority will designate contingency editions (paragraph A2.14) and inform members, SA-ALC/LTMKK and DIRNSA/Y13.

NOTE: NSA establishes supersession rates based on security, operational need, production and resupply constraints. Except in emergencies, controlling authorities cannot change supersession rates.

A2.6. Operational Requirement. Controlling authorities must know the operational requirements supported by the cryptonet and the proper use of the key. Controlling authorities must keep familiar with the operation and capabilities of the associated equipment.

A2.7. HJ Time. Controlling authorities specify HJ time for the cryptonet, except where specified in the material. Keep the time selected for HJ consistent throughout the cryptonet. Additionally, the time chosen must have the least operational impact.

A2.8. Cryptonet Configuration. Controlling authorities notify all cryptonet members, SA-ALC/LTMKK, and DIRNSA/Y13 of any changes in cryptonet configuration or keying material status. If manual cryptosystems are concerned, controlling authorities must also notify DIRNSA/V33.

A2.9. Spare Group Assignment. Controlling authorities make temporary spare group assignments of operations codes, as necessary, and report permanent spare group assignments to HQ AFC4A/SYS, who makes sure they are included in future production copies.

A2.10. Key Distribution. Controlling authorities prescribe electronic generation and distribution of keys (except key encryption keys (KEK)). They also prescribe physical transfer of keys in a common fill device, or local reproduction of keys, when established channels cannot supply the material in time to meet urgent operational requirements. Controlling authorities make sure reproduced material is kept to the minimum essential amount and is properly classified, controlled, and destroyed as applicable. Controlling authorities obtain register numbers from SA-ALC/LTMKK for copies of Accounting Legend Code-1 reproduced by Air Force COMSEC accounts. The COMSEC account may obtain register numbers for reproductions of unsealed manual cryptosystems (codes and authenticators) from SA-ALC/LTMKK. Controlling authority approval is required for reproduction of sealed manual cryptosystems. Controlling authorities who routinely allow reproduction of the same material should increase the copy count of that material.

A2.11. Extracts. Controlling authorities approve the number of extracts of keying material issued to a user at any one time, except where specified in the material. Control and destroy extracts in the same manner as complete COMSEC documents.

NOTE: Approving the issuance of extracts from protectively packaged keying material defeats the purpose of the protective packaging and increases the vulnerability of the key contained inside. Issue protectively packaged keying material as entire editions, except where operational necessity prevents such issue.

A2.12. Defective Keying Material. Controlling authorities report defective keying material (AFI 33-212) by message to DIRNSA/Y265/Y132, with an information copy to SA-ALC/LTMKK. Send message to DIRNSA/V51A if there is evidence of tampering, otherwise, send message to DIRNSA/Y132. Describe what is wrong with the material, if known, or reason for submitting the report. Furnish all available information to aid NSA in analyzing the problem. Keep defective material and all associated packaging materials until disposition instructions are received. Return recalled keying material by the Defense Courier Service, Department of State Courier System, or by cleared department, agency, or contract courier. Transfer reports must state reason for return. Refer to the recall message and include any other remarks requested in the recall message.

A2.13. Keying Material Revalidations. Controlling authorities begin and carry out annual revalidation of keying material, used with machine cryptosystems, to confirm cryptonet structure, quantities and adequacy of the key to meet operational requirements, and continuing requirement for the key. Deactivate the cryptonet if no longer needed. During the revalidation, identify cryptosystems of low peacetime use that are candidates for placement into contingency status (paragraph A2.14). Revalidate keying material for manual cryptosystems according to AFI 33-216. Send a summary of each revalidation to SA-ALC/LTMKK.

A2.14. Designating Contingency Keying Material. You may designate keying material for contingency use when large amounts of unused keying material, provided for regular consumption, are scheduled for destruction. Hold contingency keying material for a specific, yet irregular, requirement. Activate the material when needed for the specific requirement, and destroy after use. Substantial savings in production, distribution, accounting, and destruction are realized when contingency materials are used instead of regularly superseded effective key. Controlling authorities recommend keying material for contingency designation to SA-ALC/LTMKK and DIRNSA/Y13.

A2.15. Tactical and High Risk Situations.

A.2.15.1. Tactical Situations. Issue keying material in ample quantities to support mission requirements. You may issue it in either hard copy or electronic form depending on the risk, as determined by the local commander. Use any multiple key storage capacity of the equipment.

If equipment does not have multiple fill capacity, or has insufficient capacity, issue common fill or approved key transfer devices. If hard copy keying material is issued, issue extracts when only a few settings are required; otherwise issue the entire

edition. Base your decision of whether to issue extracts or entire editions on a risk assessment and careful consideration of the logistic problems associated with emergency resupply due to compromise.
A2.15.2. High Risk Situations. Issue key in electronic form.

A2.16. Reproduction of Manual Cryptomaterial. You may locally copy manual cryptosystems (that is, codes and authenticators) as necessary to meet operational needs. Controlling authority approval is not required, but you may only issue copied material to users validated by the controlling authority. Obtain register numbers of ALC 1 material from SA-ALC/LTMKK, and pick up and account for the reproduced material according to AFKAG-2, *Air Force COMSEC Accounting Manual*.

ROLE OF THE NATIONAL SECURITY AGENCY

A3.1. NSA performs the following COMSEC keying material oversight functions:
A3.1.1. Performs controlling authority functions for specified material including, but not limited to, all FIREFLY keying material generated by NSA facilities.
A3.1.2. Takes or recommends appropriate action when COMSEC material has been subjected to compromise and lets appropriate authorities know of such actions.
A3.1.3. Assists controlling authorities in their annual cryptonet review, when requested.
A3.1.4. Advises controlling authorities of the logistic impact of compromise, supersession, or other controlling authority decisions, in coordination with the appropriate distribution authorities.

GUIDELINES FOR EXTENDING CRYPTOPERIODS

A4.1. When you must extend cryptoperiods for reasons other than logistics needs (for example, under pre-strike, battlefield, or field training conditions), controlling authorities are encouraged to conduct a risk assessment prior to implementing the extension. Controlling authorities should consider the following factors before making a decision as to the length of time the cryptoperiod will be extended:

A4.1.1. Size of the Cryptonet. The key used on a large cryptonet is usually more vulnerable to compromise than the key used on a small cryptonet because it is available at more locations and more people have access to it. Also, large nets generally carry higher volumes of traffic than small nets. The compromise of a key used to secure a large net could make more intelligence available to an adversary. (For this reason, controlling authorities must keep their cryptonets as small as operationally feasible.)

A4.1.2. Location and Operating Environment of Net Members. Net members located in the United States, its territories, and its protectorates are normally at less risk than those in other locations. Net members located in high risk environments (that is, areas outside the United States where there is a small or no United States or allied military presence or where the political climate is unstable) have an increased risk of physical compromise. Mobile and tactical users have a greater opportunity for loss (particularly undetected loss) of material than do fixed plant net members. In addition, loss on the battlefield could pose an immediate threat not only to United States communications but also to United States lives.

A4.1.3. Sensitivity and Perishability of Traffic. The controlling authority should consider the classification of the protected information, and whether the information is of long -or- short term intelligence value. Compromise of a key used to secure upper level strategic communications would have a more devastating effect on United States security than would compromise of a key used to secure highly perishable or lower level tactical communications.

A4.1.4. Emergency Supersession Plan. The controlling authority must have a plan for replacing compromised key. They must know approximately how quickly they can replace the key if the plan is realistic in a worst case scenario. The controlling authority should test their plan, because it is extremely difficult to accomplish an unscheduled rekey in a large net without creating additional problems and confusion. The controlling authority must know the logistic channels that support the cryptonet as well as the electronic key transfer or distribution capabilities of the associated equipment.

A4.1.5. Operation Impact of an Extended Cryptoperiod. The controlling authority must make an assessment as to whether extending the cryptoperiod is for operational necessity or for operator convenience. If we do not follow standard procedures during wartime, the value of our peacetime training is questionable. Also, feedback from personnel involved in recent military operations has revealed that operators were confused by changes in operational procedures during the stress of a wartime environment.

A4.2. If cryptoperiod extensions are necessary to maintain critical communications during battle (actual or field training), the following guidelines apply:

A4.2.1. Begin all preplanned cryptoperiods with a new key setting.

A4.2.2. Extend cryptoperiods by net and not by short title, whenever possible.

A4.2.3. Rekey all affected nets as soon as there is a break in activity.